



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07200433 A**(43) Date of publication of application: **04.08.95**

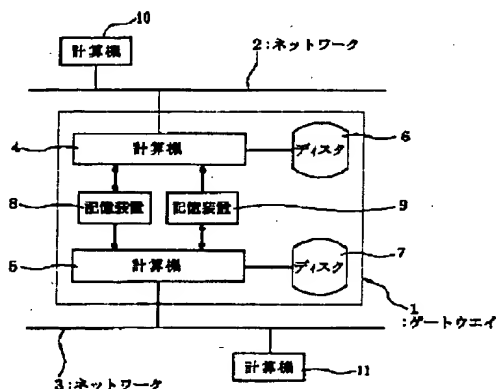
(51) Int. Cl.

G06F 13/00
H04L 12/66
(21) Application number: **06012099**(71) Applicant: **FUJI FACOM CORP**(22) Date of filing: **07.01.94**(72) Inventor: **SHIROKURA YOSHIZUMI**(54) **GATEWAY**

(57) Abstract:

PURPOSE: To improve the security by preventing illegal invasion among networks.

CONSTITUTION: A couple of storage devices 8 and 9 where writing in mutually opposite directions is restricted are provided, and transfer data sent from a computer 10 to a computer 4 are written in the storage device 8. A computer 5 takes data out of the storage device 8 and sends them to a computer 11 at a transfer destination. Flag data for erasing data in the storage device 8 which are already processed by the computer 4 are generated by the computer 5 and written in the storage device 9. The computer 4 erases the object data in the storage device 8 on the basis of the flag data in the storage device 9. Then the computer 5 checks whether or not the data corresponding to the flag data are erased and then erases the flag data on condition that the data have been erased.



COPYRIGHT: (C)1995,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-200433

(43) 公開日 平成7年(1995)8月4日

(51) Int.Cl.⁹

G 0 6 F 13/00

H 0 4 L 12/66

識別記号

3 5 3 C 7368-5B

庁内整理番号

8732-5K

F I

H 0 4 L 11/20

技術表示箇所

B

審査請求 未請求 請求項の数 1 F D (全 4 頁)

(21) 出願番号

特願平6-12099

(22) 出願日

平成6年(1994)1月7日

(71) 出願人 000237156

富士ファコム制御株式会社

東京都日野市富士町1番地

(72) 発明者 白倉 善積

東京都日野市富士町1番地 富士ファコム

制御株式会社内

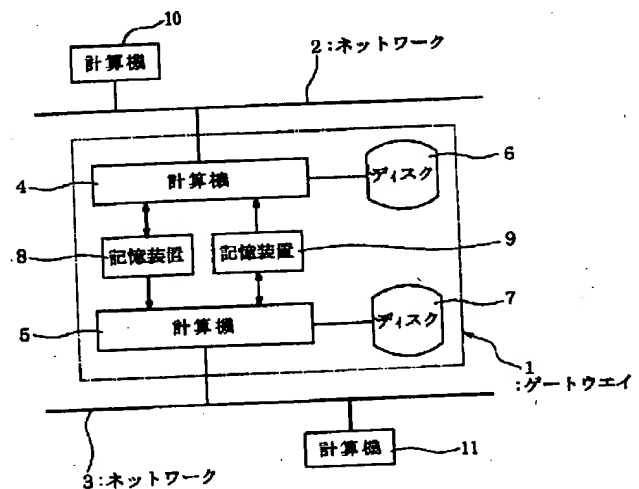
(74) 代理人 弁理士 森田 雄一

(54) 【発明の名称】 ゲートウェイ

(57) 【要約】

【目的】 ネットワーク間の不法侵入を防止してセキュリティを高める。

【構成】 互いに反対方向の書込みを制限した1対の記憶装置8、9を備えておき、計算機10から計算機4へ送られた転送データを記憶装置8へ書き込む。計算機5は記憶装置8内のデータを取り出して転送先の計算機1へ送信する。記憶装置8内の処理済みのデータを計算機4により消去するためのフラグデータを、計算機5が作成して記憶装置9内に書き込む。計算機4は、記憶装置9のフラグデータに基づき記憶装置8内の消去対象データを消去する。次に、計算機5はフラグデータに対応するデータが消去されたか否かを調べ、消去されていればそのフラグデータを消去する。



【特許請求の範囲】

【請求項1】 それぞれのネットワークごとに設置された転送データメモリと、
両ネットワークの間に設置されて両ネットワーク側からのリード・ライトが可能な共有メモリと、
それぞれのネットワークごとに設置され、送信先が他のネットワークである転送データを自ネットワークから受信して転送データメモリに格納する手段と、
それぞれのネットワークごとに設置され、転送データメモリに格納されている転送データを読み取り共有メモリに書き込む手段と、
それぞれのネットワークごとに設置され、共有メモリに書き込まれている自ネットワーク宛の転送データを読み取り自ネットワーク上の送信先へ送信する手段と、
を備えたゲートウェイにおいて、
前記共有メモリを、一方のネットワーク側からはリードライトを可能としかつ他方のネットワーク側からはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワーク側からはリードオンリとした共有メモリとにより構成するとともに、
それぞれのネットワークごとに設置され、転送データが読み取られて送信された後にリードオンリの共有メモリに残った転送データを消去するためのフラグデータを作成してリードライト可能な共有メモリに書き込む手段と、
それぞれのネットワークごとに設置され、リードオンリの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データを消去する手段と、
それぞれのネットワークごとに設置され、リードライト可能な共有メモリとリードオンリの共有メモリを比較して、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンリの共有メモリにない場合は、そのフラグデータをリードライト可能な共有メモリから消去する手段と、
を備えたことを特徴とするゲートウェイ。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、ゲートウェイに関し、詳しくは異なるネットワーク間でのリモートアクセスを不可能にしてセキュリティを高めたゲートウェイに関する。

【0002】

【従来の技術】 従来のゲートウェイは異なるネットワーク間に共通な記憶装置を設けて、相互間のデータ転送を行っている。

【0003】

【発明が解決しようとする課題】 しかしながらこれら従来のゲートウェイでは、ソフトウェアの設定を誤ると、

一方のネットワークの端末が保持する秘密情報を他方のネットワークの端末に転送可能な場合が発生するという問題があった。本発明は上記問題点を解決するためになされたもので、その目的とするところは、ネットワーク間のセキュリティを高めて、秘密情報が誤ってゲートウェイを通過して他のネットワークに転送されることのないようにしたゲートウェイを提供することにある。

【0004】

【課題を解決するための手段】 上記目的を達成するために、本発明は、それぞれのネットワークごとに設置された転送データメモリと、両ネットワークの間に設置されて両ネットワーク側からのリード・ライトが可能な共有メモリと、それぞれのネットワークごとに設置され、送信先が他のネットワークである転送データを自ネットワークから受信して転送データメモリに格納する手段と、それぞれのネットワークごとに設置され、転送データメモリに格納されている転送データを読み取り共有メモリに書き込む手段と、それぞれのネットワークごとに設置され、共有メモリに書き込まれている自ネットワーク宛の転送データを読み取り自ネットワーク上の送信先へ送信する手段とを備えたゲートウェイにおいて、前記共有メモリを、一方のネットワーク側からはリードライトを可能としかつ他方のネットワーク側からはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワーク側からはリードオンリとした共有メモリとにより構成するとともに、それぞれのネットワークごとに設置され、転送データが読み取られて送信された後にリードオンリの共有メモリに残った転送データを消去するためのフラグデータを作成してリードライト可能な共有メモリに書き込む手段と、それぞれのネットワークごとに設置され、リードオンリの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データを消去する手段と、それぞれのネットワークごとに設置され、リードライト可能な共有メモリとリードオンリの共有メモリを比較して、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンリの共有メモリにない場合は、そのフラグデータをリードライト可能な共有メモリから消去する手段とを備えたことを特徴とする。

【0005】

【作用】 本発明においては、ゲートウェイの共有メモリが、一方のネットワーク側からはリードライトを可能としかつ他方のネットワーク側からはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワーク側からはリードオンリとした共有メモリとにより構成される。それぞれのネットワークごとに、転送データが読み取られて転送データメモリに書き込まれた後に、リードオンリの共有メモリに残った転送データを消去するためのフラグデータが作

成されてリードライト可能な共有メモリに書き込まれる。

【0006】それぞれのネットワークごとに、リードオンの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データが消去される。それぞれのネットワークごとに、リードライト可能な共有メモリとリードオンの共有メモリが比較され、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンの共有メモリにない場合は、そのフラグデータがリードライト可能な共有メモリから消去される。これら手順により、ネットワーク間ではデータの転送方向に応じて異なる共有メモリを介してデータ転送がなされることにより、一方のネットワークの端末から他方のネットワークの端末に対してリモート・アクセスすることが不可能になる。

【0007】

【実施例】以下、図に沿って本発明の実施例を説明する。図1は本発明の実施例を示すブロック図である。図において、1はゲートウェイであり、異なるネットワーク2, 3の間に接続されている。ゲートウェイ1は、計算機4, 5、転送データメモリであるところのディスク6, 7、共有メモリであるところの記憶装置8, 9から構成されている。記憶装置8は計算機4からのリード/ライト(RW)が可能であり、計算機5からはリードオンリ(RO)である。同じく、記憶装置9は計算機5からのリード/ライト(RW)が可能であり、計算機4からはリードオンリ(RO)である。

【0008】次に、ネットワーク2上の端末である計算機10から、ゲートウェイ1を介してネットワーク3上の端末である計算機11へデータ転送する場合について説明する。まず、計算機10から転送先情報を付加した転送データがネットワーク2を介して、ゲートウェイ1内の計算機4へ送られる。計算機4は送られた転送データをいったんディスク6へ格納する。次に、計算機4は一定間隔で起動される監視プログラムにより、ディスク6を調べ、転送すべきデータがある場合は、そのデータを転送先情報とデータ本体の2つに分けて記憶装置8へ移動し、移動完了後にディスク6内のデータを削除する。

【0009】一方、データを受け取る計算機5は、一定間隔で起動される監視プログラムにより、記憶装置8内を調べ、処理すべきデータがある場合は、記憶装置8からデータとその制御データを読み取り制御データ内に記述されている転送先である計算機11へネットワーク3を介して送信する。ここまでは従来のゲートウェイとほぼ同様なデータ転送手順である。しかし、記憶装置8が計算機5からはリードオンリであるため、計算機5に転送データが読み取られても、消去されることがない。そのため、ネットワーク2からデータが転送されてくるた

びに記憶装置8には処理済みの転送データが増えてしまう。

【0010】そこで、記憶装置8内の処理済みのデータを計算機4により消去してもらうことを依頼するためのフラグデータを計算機5が作成して記憶装置9内に書き込む。計算機4は記憶装置9を監視しフラグデータがある場合は、そのフラグデータに基づき消去対象データが記憶装置8内にあるか否かを調べ、ある場合はそのデータおよび対応する制御データを消去する。次に、記憶装置9に残った使用済みのフラグデータを消去するため、計算機5は監視プログラムにより、記憶装置9にあるフラグデータに対応するデータおよび対応する制御データが記憶装置8内にあるか否かを調べ、ない場合はそのフラグデータは用済みであるので消去する。これら一連の処理により、記憶装置8内の転送済みの不要データが逐次消去されて、次のデータの書き込みエリアが確保される。

【0011】なお、ネットワーク3上の計算機11からゲートウェイ1を介してネットワーク2上の計算機10へデータ転送をしようとする場合は、上述した手順を逆方向に実行することにより同様に転送される。このゲートウェイ1は、上述したように、データの転送方向によって、ネットワーク2, 3間を接続する記憶装置8と記憶装置9のいずれかを限定して使用するため、一方のネットワークの計算機から他方のネットワークの計算機に対してのリモート・アクセス(リモート・コピー、リモート・シェルの実行等)を不可能にしてネットワーク経由の不法侵入を防止し、ネットワーク間のセキュリティを向上することができる。

【0012】

【発明の効果】以上述べたように本発明によれば、共有メモリを一方のネットワーク側からはリードライトを可能としかつ他方のネットワークからはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワークからはリードオンリとした共有メモリとにより構成して、データの転送方向に応じて異なる共有メモリを介してデータ転送が行われる。それにより、一方のネットワークの端末から他方のネットワークの端末に対してリモート・アクセスすることが不可能となり、ネットワーク経由の不法侵入が防止されてネットワーク間のセキュリティが向上する。

【図面の簡単な説明】

【図1】本発明の実施例の構成を示すブロック図である。

【符号の説明】

- 1 ゲートウェイ
- 2, 3 ネットワーク
- 4, 5 計算機
- 6, 7 ディスク
- 8, 9 記憶装置

10, 11 計算機

5

6

【図1】

